JOURNAL OF NUMBER THEORY 13, 116–121 (1981)

Kronecker's Theorem and Lehmer's Problem for Polynomials in Several Variables*

DAVID W. BOYD

Department of Mathematics, The University of British Columbia, Vancouver V6T 1W5, Canada

Communicated by H. L. Montgomery

Received September 5, 1979

Mahler defined the measure of a polynomial in several variables to be the geometric mean of the modulus of the polynomial averaged over the torus. The classical theorem of Kronecker which characterizes monic polynomials with integer coefficients all of whose roots are inside the unit disk can be regarded as characterizing those polynomials of one variable whose measure is exactly 1. Here this result is generalized to polynomials in several variables. The method employed also gives· easy generalizations of recent results of Schinzel and Dobrowolski on Lehmer's problem.

If $F(z)$ is a polynomial with complex coefficients then the measure of F is defined by

$$M(F) = |a_o| \prod_{i=1}^{k} \max(|\alpha_i|, 1), \tag{1}$$

where a_o is the leading coefficient and $\alpha_1,..., \alpha_k$ are the roots of F. If F has integer coefficients then (1) shows that $M(F) \geqslant 1$ and a classical theorem of Kronecker [5] characterizes those F with $M(F) = 1$ as being of the form $\pm z^h K(z)$, where K is cyclotomic (not necessarily irreducible).

Lehmer [6] asked whether there is a positive constant $\varepsilon_0 > 0$ so that, if $M(F) > 1$ then $M(F) \geqslant 1 + \varepsilon_0$. This has not yet been settled but Blanksby and Montgomery [1], Stewart [10] and Dobrowolski [3] have given lower bounds depending on the degree of F while Schinzel [9] has given a bound dependent on the number of non-zero coefficients and the height of F, and Dobrowolski [4] has given a bound dependent only on the number of non-zero coefficients.

* This work was supported in part by NSERC Grant A8128.

0022-314X/81/010116–06$02.00/0

For a polynomial $F(\mathbf{z}) = F(z_1, \ldots, z_n)$ in n variables, Mahler defined $M(F)$ by

$$M(F) = \exp\left\{\int_{T^n} \log |F(\mathbf{z})| \, d\mathbf{t}\right\}, \tag{2}$$

where $\mathbf{z} = e(\mathbf{t}) = (\exp 2\pi i t_1, \ldots, \exp 2\pi i t_n)$ and T^n denotes the torus $\{\mathbf{z}\colon |z_i| = 1,\ 1 \leqslant i \leqslant n\}$ parameterized by $0 \leqslant t_i < 1$, for $1 \leqslant i \leqslant n$. Jensen's formula shows that (1) and (2) are equivalent if $n = 1$. Our Lemma 2 gives further reasons for the belief in the "correctness" of Mahler's definition.

Writing $F(\mathbf{z}) = a_0(z_1, \ldots, z_{n-1})\, z_n^k + \cdots + a_k(z_1, \ldots, z_{n-1})$, we see from (1) that $M(F) \geqslant M(a_0)$ and then by induction that if F has integer coefficients then $M(F) \geqslant 1$. In this paper we generalize Kronecker's theorem by characterizing those $F(z_1, \ldots, z_n)$ with integer coefficients for which $M(F) = 1$. To do this, we exploit a connection between the several variable polynomial $F(z_1, \ldots, z_n)$ and the set of single variable polynomials $F(z^{r_1}, \ldots, z^{r_n})$. The key result is our easily proved Lemma 2, which is used in combination with some rather deep results of Schinzel [9]. Lemma 2 allows us to obtain rather easily generalizations of the results of Schinzel [9] and Dobrowolski [4] to several variables.

Montgomery and Schinzel [8] made use of this transformation to obtain a several variables version of Kronecker's theorem, characterizing those F in $\mathbb{Z}[z_1, \ldots, z_n]$ with $F(\mathbf{0}) = 1$ which do not vanish in the polydisk $\{\mathbf{z}\colon |z_i| < 1\}$. This does not give the complete set of F with $M(F) = 1$ as examples such as $z_1 + z_2$ indicate.

Definitions. If $F(z_1, \ldots, z_n)$ is a polynomial with complex coefficients, we write $k(F)$ for the number of non-zero coefficients of F and $H(F)$ for the maximum of the absolute values of the coefficients of F.

As in [9] we define an *extended cyclotomic polynomial* to be one of the form $\psi(\mathbf{z}) = z_1^{b_1} \cdots z_n^{b_n} \Phi_m(z_1^{v_1} \cdots z_n^{v_n})$, where $\Phi_m(z)$ is the mth irreducible cyclotomic polynomial, the v_i are a set of coprime integers and $b_i = \max(0, -v_i \deg \Phi_m)$ is chosen minimally so that $\psi(\mathbf{z})$ is a polynomial in z_i.

For each n, we define K_n to be the set of polynomials which are products of $\pm z_1^{c_1} \cdots z_n^{c_n}$ and extended cyclotomic polynomials.

Theorem 1. *Suppose that $F(z_1, \ldots, z_n)$ is a polynomial with integer coefficients; then $M(F) = 1$ if and only if F is an element of K_n.*

Theorem 2. *Suppose that there is a function $c(k, H) > 1$ such that if $P(z)$ has integer coefficients and $M(P) > 1$ then $M(P) \geqslant c(k(P), H(P))$. Then the same result holds for polynomials in any number of variables; that is, if $F(z_1, \ldots, z_n)$ has integer coefficients and $M(F) > 1$ then $M(F) \geqslant c(k(F), H(F))$.*

PRELIMINARY LEMMAS

An important role in our proofs will be played by the following function: for $\mathbf{r} \in \mathbb{Z}^n$, define

$$\mu(\mathbf{r}) = \min\{H(\mathbf{v}): \mathbf{v} \in \mathbb{Z}^n, \mathbf{v} \neq \mathbf{0} \text{ and } \mathbf{v} \cdot \mathbf{r} = 0\},$$

where $H(\mathbf{v}) = \max(|v_1|,\dots, |v_n|)$. We note for future reference that there are $\mathbf{r} \in \mathbb{Z}^n$ for which $\mu(\mathbf{r})$ is arbitrarily large. For example, if $\mathbf{r} = (1, m,\dots, m^{n-1})$ then $\mu(\mathbf{r}) = m$. To see this, observe that $\mu(\mathbf{r}) \leqslant m$ since $\mathbf{v}_0 = (m, -1, 0,\dots, 0)$ satisfies $\mathbf{v}_0 \cdot \mathbf{r} = 0$, and if on the other hand $\mathbf{v} \cdot \mathbf{r} = 0$ and k is the greatest index with $v_k \neq 0$, then

$$-v_k m^{k-1} = v_1 + v_2 m + \cdots + v_{k-1} m^{k-2}$$

so that $m^{k-1} \leqslant |-v_k m^{k-1}| \leqslant H(\mathbf{c})(m^{k-1} - 1)/(m-1)$ so $H(\mathbf{v}) > m-1$.

If $F(z_1,\dots, z_n)$ is a polynomial and $\mathbf{r} \in \mathbb{Z}^n$, we define

$$F_{\mathbf{r}}(z) = z^h F(z^{r_1},\dots, z^{r_n}), \tag{3}$$

where h is the smallest integer which makes the right member of (3) a polynomial in z.

Observe that if we write $F(z_1,\dots, z_n) = \sum_{\mathbf{j}\in J} a(\mathbf{j})\, z_1^{j_1} \cdots z_n^{j_n}$, where J is a finite subset of $\mathbb{Z}^n$ then $F_{\mathbf{r}}(z) = z^h \sum_{\mathbf{j}\in J} a(\mathbf{j})\, z^{\mathbf{j}\cdot\mathbf{r}}$ so that if $d = \max\{H(\mathbf{j}_1 - \mathbf{j}_2)$: $\mathbf{j}_1, \mathbf{j}_2 \in J\}$, then for $\mu(\mathbf{r}) > d$ no two of the exponents $\mathbf{j} \cdot \mathbf{r}$ can be equal and hence $H(F_{\mathbf{r}}) = H(F)$ and $k(F_{\mathbf{r}}) = k(F)$.

LEMMA 1. *Suppose that $f(\mathbf{t})$ is a continuous function on the torus T^n. Then*

$$\lim_{\mu(\mathbf{r})\to\infty} \int_T f(s\mathbf{r})\, ds = \int_{T^n} f(\mathbf{t})\, d\mathbf{t}.$$

More precisely, there is a function $\varepsilon(\mu)$ (depending on f) which tends to 0 as $\mu \to \infty$ such that, for all $\mathbf{r} \in \mathbb{Z}^n$,

$$\left| \int_T f(s\mathbf{r})\, ds - \int_{T^n} f(\mathbf{t})\, d\mathbf{t} \right| < \varepsilon(\mu(\mathbf{r})).$$

Proof. By Weierstrass' approximation theorem, it suffices to prove the result for trigonometric polynomials. Thus we may assume that

$$f(\mathbf{t}) = \sum_{\mathbf{m}} c(\mathbf{m})\, e(\mathbf{m} \cdot \mathbf{t}),$$

where the sum is over a finite set of $\mathbf{m} \in \mathbb{Z}^n$, and as usual $e(\theta) = \exp(2\pi i\theta)$. Then

$$\int_T f(s\mathbf{r})\, ds = \sum_{\mathbf{m}\cdot\mathbf{r}=0} c(\mathbf{m}) = c(\mathbf{0}) + \sum \{c(\mathbf{m}) \colon \mathbf{m}\cdot\mathbf{r} = 0, \mathbf{m} \neq 0\}$$

$$\to c(\mathbf{0}) = \int_{T^n} f(\mathbf{t})\, dt$$

as $\mu(\mathbf{r}) \to \infty$ since the set $\{\mathbf{m} \colon \mathbf{m}\cdot\mathbf{r} = 0,\ \mathbf{m} \neq 0\}$ contains only vectors with $H(\mathbf{m}) \geqslant \mu(\mathbf{r})$.

LEMMA 2. *Let $F(z_1,\dots, z_n)$ be a polynomial with complex coefficients. Then*

$$\limsup_{\mu(\mathbf{r})\to\infty} M(F_\mathbf{r}) \leqslant M(F). \tag{4}$$

In fact, if $F(z_1,\dots, z_n) \neq 0$ on T^n then

$$\lim_{\mu(\mathbf{r})\to\infty} M(F_\mathbf{r}) = M(F). \tag{5}$$

Proof. For any $\delta > 0$, $\log(|F(\mathbf{z})| + \delta)$ is continuous on T^n. Thus, by Lemma 1,

$$\lim_{\mu(\mathbf{r})\to\infty} M(|F_\mathbf{r}| + \delta) = M(|F| + \delta).$$

Since $M(F_\mathbf{r}) \leqslant M(|F_\mathbf{r}| + \delta)$ for all $\delta > 0$, we thus have

$$\limsup_{\mu(\mathbf{r})\to\infty} M(F_\mathbf{r}) \leqslant M(|F| + \delta).$$

Letting δ decrease to 0 and using monotone convergence, we obtain (4).

The final result (5) is a direct consequence of Lemma 1.

Remark. We conjecture that in fact (5) holds for all polynomials, without the condition $F(\mathbf{z}) \neq 0$ on T^n. We have proved this in case $n = 2$ [2] by an argument which makes strong use of the fact that F is a polynomial, in contrast to the above proof, which only uses the continuity of F.

LEMMA 3 (Schinzel). *Suppose that $F(z_1,\dots, z_n)$ is a polynomial with integer coefficients but that $F \notin K_n$. Then there is a constant $c(F)$ such that if $F_\mathbf{r} \in K_1$ then $\mathbf{v}\cdot\mathbf{r} = 0$ for some $\mathbf{v} \in \mathbb{Z}^n$ with $0 < H(\mathbf{v}) < c(F)$.*

Proof. If $F \notin K_n$, then there is an irreducible factor G of F which is not in K_n. By hypothesis, either $G_\mathbf{r}$ contains a cyclotomic factor or else $G_\mathbf{r}$ is identically 1. In the first case Lemma 3 of [9] applies to assert the existence of a suitable constant while in the second case considerations such as those preceding Lemma 1 apply.

LEMMA 4 (Schinzel). *Suppose that* $F(z)$ *has integer coefficients and* $F \notin K_1$. *Then*

$$M(F) \geqslant 1 + \exp(-H \exp_k 2k^2),$$

where $H = H(F)$, $k = k(F)$ *and* $\exp_k$ *denotes the k-fold iterated exponential.*

Proof. This is the main result of [9].

Proof of Theorem 1. If $F \in K_n$ then clearly $M(F) = 1$.

Conversely, assume $M(F) = 1$ but that $F \notin K_n$. Let $\mathbf{r}$ be such that $\mu(\mathbf{r}) > d$ so that $H(F_{\mathbf{r}}) = H(F)$ and $k(F_{\mathbf{r}}) = k(F)$. Then by Lemma 4, there is a constant $\eta > 0$ so that if $F_{\mathbf{r}} \notin K_1$ then $M(F_{\mathbf{r}}) > 1 + \eta$. By Lemma 2, $\limsup M(F_{\mathbf{r}}) \leqslant M(F) = 1$ so for $\mu(\mathbf{r})$ sufficiently large we must have $M(F_{\mathbf{r}}) < 1 + \eta$ and hence $F_{\mathbf{r}} \in K_1$. But by Lemma 3, if $\mu(\mathbf{r}) \geqslant c(F)$ then $F_{\mathbf{r}} \in K_1$ implies $F \in K_n$. Since we are free to choose $\mu(\mathbf{r})$ arbitrarily large, this proves the theorem.

Proof of Theorem 2. If $M(F) > 1$ then by Lemma 3 and Theorem 1, $M(F_{\mathbf{r}}) > 1$ for $\mu(\mathbf{r}) \geqslant c(F)$. Thus $M(F_{\mathbf{r}}) \geqslant c(k(F_{\mathbf{r}}), H(F_{\mathbf{r}}))$, by hypothesis. But $k(F_{\mathbf{r}}) = k(F)$ and $H(F_{\mathbf{r}}) = H(F)$ for $\mu(\mathbf{r})$ sufficiently large, and $M(F) \geqslant \limsup M(F_{\mathbf{r}})$ by Lemma 2. Thus letting $\mu(\mathbf{r}) \to \infty$ completes the proof.

Note added in proof. A. Schinzel informs me that [4] and [9] will appear together in a joint paper of E. Dobrowolski, W. Lawton, and A. Schinzel, "On a problem of Lehmer," *Acta Math. Acad. Sci. Hung.*, to appear. W. Lawton has independently proved Theorem 1 by a rather different method in "A generalization of a theorem of Kronecker," *Journal of the Science Faculty of Chiangmai University* (Thailand), **4** (1977), 15–23. A third proof of Theorem 1 has recently been obtained by C. J. Smyth, "A Kronecker-type theorem for complex polynomials in several variables," *Canad. Math. Bull.*, to appear.

REFERENCES

1. P. E. BLANKSBY AND H. L. MONTGOMERY, Algebraic integers near the unit circle, *Acta Arith.* **28** (1971), 355–369.
2. D. W. BOYD, Pisot numbers and the width of meromorphic functions, privately circulated manuscript, January 1977.
3. E. DOBROWOLSKI, On a question of Lehmer and the number of irreducible factors of a polynomial, *Acta Arith.* **34** (1979), 391–401.
4. E. DOBROWOLSKI, On a question of Lehmer, to appear.
5. L. KRONECKER, Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten, *J. Reine Angew. Math.* **53** (1857), 173–175.

6. D. H. LEHMER, Factorization of certain cyclotomic functions, *Ann. of Math.* (2) **34** (1933), 461–479.
7. K. MAHLER, On some inequalities for polynomials in several variables, *J. London Math. Soc.* **37** (1962), 341–344.
8. H. L. MONTGOMERY AND A. SCHINZEL, Some arithmetic properties of polynomials in several variables, *in* "Transcendence Theory: Advances and Applications" (A. Baker and D. W. Masser, Eds.), pp. 195–203, Academic Press, New York, 1977.
9. A. SCHINZEL, On a problem of Lehmer, *Acta Math. Acad. Sci. Hungar.*, in press.
0. C. L. STEWART, Algebraic integers whose conjugates lie near the unit circle, *Bull. Soc. Math. France* **106** (1978), 169–176.

Printed in Belgium